PERSPECTIVES

a CANADIAN SECURITY INTELLIGENCE SERVICE publication

Report # 2001/11

INFORMATION OPERATIONS

This paper uses open sources to examine any topic with the potential to cause threats to public safety or national security.

Introduction

1. With the advent of the personal desktop computer in 1980, the manner in which the public and private sectors conduct business and provide services to the public at large has changed. Over time, millions of computers and thousands of dissimilar networks worldwide have been connected through a global network of networks. Internet use has more than doubled annually for the last several years to an estimated 40 million users worldwide in nearly every country today. Connections between computer systems are growing at an ever-increasing rate, with the Internet adding a new network about every 30 minutes. This is especially true as businesses are beginning to engage in e-commerce, or conduct business on-line, and governments begin to provide information and services via an electronic environment, or e-government. According to a report by the Computer Industry Almanac, nearly 43 percent of Canadians use the Internet, which makes Canada one of the leading countries for Internet use.

2. The growing dependence of governments, institutions, business, groups and individuals on computer- based communications and information technologies has resulted in a constantly changing view of what constitutes threats in today's "information age." It is no longer necessary for "hostile actors"[1] to have direct physical access to a computer to copy, destroy or manipulate data. People can use a variety of techniques and software tools to exploit a targeted system once they gain unauthorized access remotely via the Internet or by dialling directly into the system using a telephone and a modem. Most legislation and protective measures address physical attacks on critical systems and data; however, they have been or are in the process of being revised and updated to deal with the new class of computer-based threats defined as Information Operations (IO).

Information Operations

3. The concept of IO has its root in that of "Information Warfare" (IW), which is the physical and computer-based operations used by military forces in time of conflict and near-conflict to compromise the access to and viability of information received by the decision-makers of an enemy, while at the same time protecting their own information and information systems. The term IO is used to denote the use of IW tools and techniques. The definition has evolved over time to reflect the need for a state to maintain national security by protecting its critical infrastructure. The critical sectors in a state's infrastructure are those of: transportation; oil and gas; water; emergency services; continuity of government services; banking and finance; electrical power; and telecommunications.

4. IO is the outgrowth of military doctrine that focussed on the use of electronic warfare measures to degrade the capabilities of adversaries on the battlefield. Operations conducted during the Desert Storm campaign in 1991 indicated that technological development had provided the military with computer-based tools and techniques that could be used to degrade not only military systems but those of government and the private sector as well.

---

[1] Hostile actors can be individuals, extremist groups, terrorist groups, criminal organizations, intelligence services or armed forces.

5. Within the realm of IO, there is no safe haven and territorial boundaries become irrelevant as IO can be conducted at any time against any sector, public or private. All other "cyber" activity, such as cybercrime[2], cyberterrorism[3], cyberwar[4], netspionage and hacktivism[5] is a subset of IO. However, most discussions relating to the use of computer-based tools and techniques in the context of IO have come to focus on information assurance and the protection of computer-based systems and networks from an intrusion or attack.

The Threat

6. Information Operations could be used to target national information systems from anywhere in the world using inexpensive hardware and software.[6] The potential threats to the critical infrastructure from a variety of hostile actors with such tools and techniques include:

- the disruption of components of the national infrastructure;
- the exploitation of information;
- the manipulation of information for political, economic, or military purposes; and
- the destruction of information or infrastructure components.

7. Degrading of the operation of, or damaging, a targeted computer system could have significant negative impacts on social, political and economic activities, which would entail serious ramifications in the area of national security. Although security measures are being created to protect these infrastructures, the development of attack tools to circumvent these protective measures is ongoing and these attack mechanisms have become freely available through the Internet. The number of intrusions into computer-based systems is on the rise and the tools used to exploit existing vulnerabilities are growing in sophistication and simplicity. Although only a small number of system intrusions are reported, indications are that the level of reported incidents and vulnerabilities is doubling annually. In 2002, statistics released by the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University in Pittsburgh show that 1,334 computer security incidents were reported worldwide in 1993, compared to 21,756 in 2000 and 52,658 in 2001.

8 The threat of unauthorized intrusions into computer systems and networks increases proportionately to the commonality of applications used and degree of connectivity to external networks like that of the Internet. The requirement for interoperability coupled with such connections create

---

[2] A crime related to technology, computers and the Internet, but more specifically, all forms of attack on automated data-processing systems.

[3] While there are a number of definitions for the term, "cyberterrorism," in the context of this paper, will be defined as premeditated, politically motivated attacks against information, computer systems, computer programs, and data which can result in violence against noncombatant targets by subnational groups or clandestine agents.

[4] A synonym for Information Warfare.

[5] Hacktivism is the act of hacking or breaking into a computer system for a politically or socially motivated purpose. It is the combination of hacking and on line activism.

[6] The National Security Agency (NSA) conducted 37 computer intrusion exercises during the past three and one-half years, and 99% of the attacks performed on American computer systems were undetected. The attack teams taking part in these exercises used only the tools and techniques that could be acquired via the Internet.

vulnerabilities that can be exploited, for whatever reason, by hostile actors, using malicious software such as viruses, Trojan Horses and worms[7] via the Internet. In addition, physical attacks like cutting power cables or destroying the hardware upon which the information infrastructure depends are the equivalent of physical denial of service (DoS) attacks. The latter form of attack prevents authorized users from gaining access to information systems and data. Any of these hostile actors can attack vulnerable infrastructure points using physical means and/or software. As a result, the growing capability of a variety of hostile actors to make offensive use of IO, in both its physical and non-physical forms, has the potential to threaten the public safety of Canadians and the national security of Canada.

9. Discussions at the United Nations on the topic of the proliferation of IO tools are couched in the rhetoric of weapons proliferation. The language has evolved from mass destruction to include IO tools and weapons of mass corruption/disruption. The increasing reliance of states on computer networks makes critical infrastructures attractive targets for attack and exploitation, and many countries have embarked on programs to develop IO doctrines and technologies.

10. According to American military and Congressional reports, Russia, China, India and Cuba have acknowledged preparations for cyberwar and are actively developing IO capabilities; North Korea, Libya, Iran, Iraq and Syria have some IO capabilities. Even though many countries are developing IO capabilities, few have the means to fully integrate various IO tools into a comprehensive attack which would cripple a country's infrastructure. However, some could develop the required abilities to mount such attacks over the next decade.

11. In his testimony before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World," 7 February 2001, Director of Central Intelligence George J. Tenet stated that new communications technologies have enabled the efforts of terrorists, who have used these technologies to advance their capabilities to raise money, spread dogma, find recruits, and plan operations. He added that some groups were acquiring rudimentary cyberattack tools. It is the Internet which helps terrorist groups adopt the model of "leaderless resistance".

Security of Systems and Data

12. The development of IO tools and techniques is evolving in pace with the rate of technological change in the communications and computer industries. The ability to communicate and connect to networks worldwide almost instantaneously has created both advantages and vulnerabilities.

13. As government departments and businesses globally have experienced both intrusions into their networks and the loss of sensitive information, they have attempted to install security measures to protect both systems and data. Unfortunately, these security packages have a short life span. Surveys and intrusion assessments conducted by private-sector security firms and by government agencies worldwide indicate that a large number of security packages and monitoring tools, many of which are commercially available, are ineffective or misconfigured. A number of surveys conducted in the United States and the

---

[7] A **Trojan Horse** is a destructive software program that masquerades as a benign application. Unlike a virus, it does not replicate itself. A **virus** is software code that reproduces itself by attaching to another program. It may damage data directly or it may degrade system performance by taking over system resources which cannot be made available to authorized users. A **worm** is a program or piece of software code that resides in distributed systems or networks. It replicates itself in order to use as much of the sytesm's resources for its own processing needs, clogging networks and computer systems as it spreads.

United Kingdom indicate that more than 80% of respondents in one case did not use firewalls or any other security measures to protect their systems and data. Up to 93% of respondents in another case were vulnerable to rudimentary attacks even if firewalls were used.

14. As more and more persons, businesses and government departments become dependent on computer-based communications and the operations of interconnected networks, the configuration of interacting computer networks and operating systems becomes more complex and creates vulnerabilities. Natural forces (like storms), the normal development of new hardware and software, and IO tools could pressure these vulnerabilities and cause failures entailing a profound effect, both short- and long-term, on the operation of government and the private sector.

15. In his testimony before a Congressional subcommittee, the Director of the Internet Security Alliance stated that 80% of all major security vulnerabilities were common to all organizations. For the most part, this is due to the use of the same vulnerable software. Generally, the ability to network has far outpaced the ability to protect these networks. The private sector, including some critical infrastructures, are installing and using wireless networks to facilitate their activities. However, many of these systems are not configured securely and are open to exploitation.

Examples of Information Operations

16. Many examples of IO-related activity can be drawn from the experience of American government departments dealing with computer intrusions and system exploitation. These experiences have been related in speeches given before Senate and Congressional committees and in documents produced by the U.S. General Accounting Office.

17. Extremist organizations, criminal groups and governments are acquiring expertise in the area of IO and could threaten various systems if they possessed the proper tools and techniques to exploit vulnerabilities, and the intent to do so. Testimony provided during committee hearings held within government in the United States revealed the fact that an increasing number of countries have or are developing offensive IO programs. Further, there is data indicating that an increasing number of extremist groups and intelligence services are becoming proficient in developing and / or using of IO tools and techniques. A number of these hostile actors may intend to use IO tools to achieve traditional threat-related activities.

18. Recent media reports indicate that protected military networks in the United States have been easily hacked using rudimentary tools. American government-sponsored examinations undertaken by the General Accounting Office indicate that software tools obtained from hacker sites on the Internet can not only degrade the operations of government departments but also threaten the critical infrastructure. A recent National Institute of Standards and Technology report highlights the fact that hackers post approximately 30 to 40 new tools on hacking sites on the Internet every month. An examination of system defacement statistics for 2001 indicates there were 22,379 Web site defacements, and out of a total 29,000 defacements recorded for the period 1998 to 22 January 2002, sites in the United States "domain" were defaced 868 times, those in the United Kingdom "domain" numbered 519, those is the

Australia "domain" totalled 345 and there were 205 defacements of sites in the Canada "domain."[8] While this type of data is incomplete, since all defacements and other system attacks are not reported, the information indicates a trend, namely that the number of system intrusions is on the rise.

19. In February 2000, national infrastructures suffered degradation from virus and distributed denial of service (DDoS) attacks. The attacks, which centred on a number of companies, each with a significant presence on the Internet, were estimated to have caused damage in the order of billions of dollars. The DDoS attacks of February 2000 acted as a proof of concept to show that a number of computers that previously had been compromised by hacker activity could be used in concert to focus attacks on a single target or on a number of targets.

20. The subsequent infestation of computers around the world with the "I Love You" virus had an even more profound effect on systems and networks. This was due in part to the fact that the phrase "I Love You" in the subject line of an e-mail message was a simple psychological operations ploy that enticed many individuals to open the virus-laden e-mail attachment and infect their computer systems. The digital threats posed by viruses, worms and Trojan Horses result in billions of damage yearly: US$17.1 billion[9] in 2000 and US$13.2 billion in 2001, according to estimates issued by the market research firm Computer Economics.

21. A 1997 Electric Power Risk Assessment conducted in the United States concluded that the power grid was riddled with vulnerabilities. Some elements of the grid used unsecured supervisory control and data acquisition (SCADA)[10] systems and were accessible through insider use of corporate local area networks (LANs). In other instances, unsecured SCADA systems could be accessed and controlled remotely via telephone. Anyone with knowledge of the phone numbers required to gain such access could affect the operation of the grid.

22. In Australia, in 2001, Vitek Boden was found guilty of using wireless technology to hack into computers that used a SCADA system to control some of the functions of a sewage treatment plant. His activities in early 2000 resulted in the release of sewage into local water systems. This was deemed to be the first recorded instance of wireless hacking. SCADA systems are used to control a variety of "critical infrastructure" processes such as electrical power distribution, natural gas delivery, and sewage and water distribution projects around the world, including those in Canada.

---

[8] These statistics are incomplete as they only represent reported defacements. Some defacements and other forms of system compromise and exploitation are not reported and/or recorded. The statistics for the various "domains" that are mentioned above do not include the ".com, .net, .org, .edu" and other non-country-specific "domains."

[9] The higher level of damage for 2000 is due to the effects of the "I Love You" virus.

[10] SCADA is a software application program used for process control, the gathering of data in real time from remote locations, and processes data in order to control equipment. SCADA systems consist of hardware and software components and provides warnings when operating conditions become hazardous. SCADA is used in power plants, oil and gas refining, telecommunications, transportation, and water and waste control.

23. Regional, political tensions have resulted in hacking duels between hacker groups and others in various countries:

- in 1999, there were hacking exchanges between China and Japan over the issue of the Nanking massacre;
- between China and Taiwan over the issue of the latter's independence of the former;
- between India and Pakistan over control of Kashmir;
- in 2000, Armenians placed false information in the Azerbaijan daily newspaper "Zerkalo;"
- the 1999-2000 tensions between Israel and Palestinians resulted in hacking activity by supporters on each side, with the activity of pro-Palestinian supporters expanding to include corporations and a pro-Israel organization in North America as targets;
- supporters of the Former Republic of Yugoslavia performed virus and denial-of-service attacks on NATO computers;
- the collision between an American surveillance plane and a Chinese fighter in April 2001 resulted in a hacking duel between the supporters of the US and China; and
- the Alqaeda Muslim Alliance - a hacker coalition composed of GForce Pakistan, the Pakistan Hackerz Club, and the Anti India Crew that appears to support Al Qaida and the Palestinian cause - hacked a number of American sites, including that of the General Accounting Office, threatening to continue attacks against Indian, American, and Israeli sites.

24. Cyberattacks tend to accompany regional tensions and/or physical attacks undertaken by hostile actors, and politically motivated computer-based attacks are increasing in volume and sophistication, and are becoming more coordinated.

Protection of the Canadian Critical Infrastructure

25. The Report of the Special Senate Committee on Security and Intelligence, published in 1999, addressed the issue of the protection of Canada's critical infrastructure. The critical infrastructure consists of both physical and cyber-based systems that are essential to the day-to-day operations of the economy and government. Historically, elements of this critical infrastructure were physically segregated. However, these elements gradually converged, became linked and became more interdependent. Advances in computer and communications technologies resulted in a growing level of automation in the operation of critical systems. The report stated that the growth of, and our increased reliance on, the critical infrastructure, combined with its complexity, has made it a potential target for physical or cyber-based terrorism.

26. In its recommendations, the Committee suggested that the government take action to protect the critical infrastructure and to:

- develop policies and resources to deal with any attacks;
- create the capability to assess and reduce infrastructure vulnerabilities, and to prevent or respond to physical and cyberattacks;
- create public sector-private sector partnerships to protect the critical infrastructure; and
- ensure that the National Counterterrorism Plan is regularly reviewed and updated, especially with respect to the impact created by new and emerging technologies that may be used by terrorists.

27. Like other countries, the Canadian government recently created a new agency designed to protect Canada's electronic infrastructure against possible cyber-based attacks and natural disasters. The new agency, the Office of Critical Infrastructure Protection and Emergency Preparedness, will report to the Minister of National Defence and will collaborate with the Solicitor General's department, the provinces and municipalities, private industry and other countries.

The Post-11 September Threat Environment

28. After the terrorist attacks of 11 September 2001, the issue of CIP changed. While the urgency of the issue has not changed, the awareness that there is an urgency has. In the United States, a number of new agencies and legislation were created to deal with "Homeland Security," a concept that has as its goal the defence of a nation's territory, critical infrastructure and population from attack. Similar antiterrorist legislation was formulated, discussed or enacted in Canada, the United Kingdom and Australia. As a corollary to this growing security awareness, information perceived as having the potential to be used by terrorists to target critical infrastructures began to be removed from a number of Web sites that provided data about critical infrastructure locations and contingency plans. Overall, greater attention is being paid to the national security ramifications of all types of cyber-based activity. What used to be viewed as an abstract threat is now viewed by some as both possible and probable.

Outlook

29. One of the greatest challenges in countering the threat in the realm of IO is that borders have become meaningless to anyone operating in a virtual environment. Even if great diligence was taken in the effort to remove vulnerabilities, it would be almost impossible to eliminate them entirely because attack tools, networks and network control systems are in a constant state of evolution.

30. As new technologies develop, so too will new attack tools and mechanisms. As a result, governments will have to set procedures in place to allow security initiatives to evolve to deal with new threats as they arise. For example, the risks associated with e-government, the movement of the private sector to an e-commerce environment, the initiatives within the private sector to provide services and system interconnection via wireless means, and the use of personal digital assistants all present challenges from a security perspective.

31. Vulnerabilities can be reduced in number but cannot be removed totally from computer-based systems. As a result, systems that are not protected in a robust manner will continue to be compromised and exploited. In general, the tools and techniques to effect such attacks on systems are becoming both easier to use and more sophisticated in their operation. A variety of hostile actors appear to be developing IO capabilities that could become significant in the near future.

Perspectives is a publication of the Research, Analysis and Production Branch of CSIS. Comments concerning publications may be made to the Director General, Research, Analysis and Production Branch at the following address: Box 9732, Stn. "T", Ottawa, Ont., K1G 4G4, or by fax at (613) 842-1312.

PERSPECTIVES

Publication du SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ

Rapport nº 2001/11

OPÉRATIONS D'INFORMATION

Ce document, inspiré de sources ouvertes, porte sur un sujet susceptible de représenter une menace pour la sécurité publique ou nationale.

Introduction

1. L'avènement de l'ordinateur personnel en 1980 a transformé la façon dont les secteurs public et privé mènent leurs activités et offrent des services à la population. Depuis, des millions d'ordinateurs et des milliers de réseaux distincts du monde entier ont été reliés, formant ainsi un immense réseau mondial de réseaux. Le nombre d'utilisateurs d'Internet a plus que doublé tous les ans au cours des dernières années et on estime aujourd'hui à quelque 40 millions le nombre d'utilisateurs répartis dans presque tous les pays. Les connexions entre systèmes informatiques augmentent à un rythme toujours plus rapide. Un nouveau réseau se branche à Internet toutes les demi-heures. Ces faits se confirment d'autant plus que les entreprises commencent à se lancer dans le commerce électronique, c'est-à-dire à faire des affaires en ligne, et que les gouvernements se mettent à offrir de l'information et des services dans un environnement électronique, le gouvernement en ligne. Selon un rapport du Computer Industry Almanac, près de 43 pour 100 des Canadiens utilisent Internet, ce qui fait du Canada l'un des chefs de file dans le domaine.

2. La dépendance croissante des gouvernements, des institutions, des entreprises, des groupes et des individus à l'égard des communications informatisées et des technologies de l'information vient sans cesse modifier la définition de la menace en cette « ère de l'information ». Les « acteurs malveillants[1] » n'ont plus besoin d'avoir directement accès à un ordinateur pour copier, détruire ou altérer les données qu'il contient. Une fois qu'un individu parvient, à distance, à s'infiltrer illégalement dans un système informatique, que ce soit au moyen d'Internet ou d'un téléphone et d'un modem, il dispose d'un large éventail de techniques et de logiciels pour l'exploiter. La plupart des lois et des mesures de protection visant à contrer les attaques contre les données et les systèmes névralgiques font maintenant l'objet de révisions et de mises à jour (si cela n'est pas déjà fait) afin de lutter contre un nouveau type de menaces informatiques, les « opérations d'information » (OI).

Opérations d'information

3. Le concept d'OI prend sa source dans celui de « guerre de l'information » (GI), à savoir les opérations physiques et informatiques menées par des forces militaires en temps de conflit et d'avant-conflit en vue de compromettre l'acheminement et la viabilité des informations nécessaires aux décideurs ennemis, tout en protégeant leurs propres informations et leurs propres systèmes. Il fait référence à l'utilisation des techniques et des outils propres à la GI. Avec le temps, la définition a évolué afin d'exprimer la nécessité pour un pays de veiller à la sécurité nationale en protégeant son infrastructure essentielle. Les secteurs névralgiques de cette infrastructure sont les suivants : transports, pétrole et gaz, eau, services d'urgence, pérennité des services gouvernementaux, opérations bancaires et financières, électricité et télécommunications.

4. Les OI découlent d'une doctrine militaire qui prône le recours à la guerre électronique pour nuire à ses adversaires sur le champ de bataille. En 1991, les opérations menées durant la campagne Tempête du désert ont permis de constater que les progrès technologiques avaient donné aux militaires des outils et des techniques informatiques capables d'endommager non seulement les systèmes militaires, mais aussi ceux du gouvernement et du secteur privé.

---

[1] Il peut s'agir d'individus, de groupes extrémistes ou terroristes, d'organisations criminelles, de services de renseignements ou de forces armées.

5. Dans le domaine des OI, nul n'est à l'abri d'une attaque et les frontières n'ont plus la moindre importance, car une opération peut être menée en tout temps contre l'un ou l'autre des secteurs, public ou privé. Toutes les « cyberactivités », telles que la cybercriminalité[2], le cyberterrorisme[3], la cyberguerre[4], le « netspionnage » et le cyberactivisme[5], constituent des sous-produits des OI. Dans ce contexte, toutefois, la plupart des débats sur l'utilisation d'outils et de techniques informatiques tournent autour de la protection des informations ainsi que des systèmes et des réseaux informatiques contre les intrusions et les attaques.

La menace

6. Du matériel et des logiciels peu coûteux[6] peuvent servir à attaquer des systèmes d'information nationaux n'importe où dans le monde. Les acteurs malveillants qui disposent d'outils et de techniques semblables peuvent représenter une menace pour l'infrastructure essentielle à plusieurs égards :

- perturbation d'éléments de l'infrastructure nationale;
- exploitation d'informations;
- manipulation d'informations à des fins politiques, économiques ou militaires;
- destruction d'informations ou d'éléments de l'infrastructure.

7. L'altération d'un système informatique donné peut avoir de graves répercussions sur les activités sociales, politiques et économiques, lesquelles peuvent nuire grandement à la sécurité nationale. Bien que des mesures de protection soient mises en oeuvre, on voit constamment apparaître de nouveaux outils capables de les contourner et il est maintenant facile de se les procurer sur Internet. Le nombre d'intrusions dans les systèmes informatiques est à la hausse et les outils servant à exploiter les points faibles des systèmes deviennent de plus en plus sophistiqués et faciles d'emploi. Le nombre d'intrusions signalées est minime, mais certains indices donnent à penser que le degré de vulnérabilité et le nombre d'incidents doublent tous les ans. Selon les statistiques publiées en 2002 par le centre de coordination de la Computer Emergency Response Team (CERT) de l'université Carnegie Mellon à Pittsburg, 1 334 incidents du genre ont été signalés dans le monde en 1993, comparativement à 21 756 en 2000 et à 52 658 en 2001.

8. Les risques d'une intrusion non autorisée augmentent suivant le nombre de connexions à des réseaux externes (Internet, par exemple) et la standardisation des applications. Ces liens, combinés au

---

[2] Crime en rapport avec la technologie, les ordinateurs et Internet; plus précisément, toute forme d'attaque contre un système informatisé de traitement de données.

[3] Bien que le terme puisse se définir de plusieurs façons, le « cyberterrorisme » se rapporte ici à toute attaque préméditée dans un but politique et dirigée contre des informations, des systèmes ou des programmes informatiques, ou des données. Il peut amener des groupes régionaux ou des agents clandestins à commettre des actes de violence contre des cibles non combattantes.

[4] Synonyme de guerre de l'information.

[5] Par cyberactivisme, on entend le piratage d'un système informatique ou son infiltration pour des raisons politiques ou sociales. La notion combine le piratage et l'activisme en ligne.

[6] Au cours des 42 derniers mois, la National Security Agency (NSA) a procédé à 37 exercices d'intrusion informatique, et 99 pour 100 de ceux réalisés sur des systèmes américains n'ont pas été détectés. Les responsables de ces attaques n'ont employé que des outils et des techniques se trouvant sur Internet.

besoin d'interopérabilité, rendent les systèmes plus vulnérables et plus susceptibles, pour de multiples raisons, d'être la cible de groupes malveillants qui utilisent des logiciels pernicieux sur Internet (virus, cheval de Troie, ver,[7] etc.). En outre, les attaques matérielles - comme le sectionnement de câbles d'alimentation ou la destruction du matériel à la base de l'infrastructure de l'information - équivalent aux attaques de déni de service. Ce type de méfait empêche les utilisateurs autorisés d'avoir accès aux systèmes d'information et aux données qu'ils contiennent. N'importe quel acteur malveillant peut exploiter les points faibles de l'infrastructure en ayant recours à des moyens matériels ou à des logiciels. Par conséquent, certains acteurs malveillants sont de plus en plus habiles pour mener des OI offensives, sous forme matérielle ou informatique, et risquent donc de représenter une menace pour la sécurité des Canadiens et la sécurité nationale.

9. Lorsqu'elles discutent de la prolifération des outils propres au OI, les Nations Unies utilisent la terminologie de la prolifération des armes. Le discours a évolué. Par armes de destruction massive, on entend maintenant les outils des OI ainsi que les armes de corruption ou de perturbation massive. En raison de la dépendance croissante des pays quant aux réseaux informatiques, leur infrastructure essentielle constitue une cible parfaite. Bon nombre de pays ont donc lancé des programmes de mise au point des outils et des technologies liées aux OI.

10. Selon des rapports de l'armée américaine et du Congrès, la Russie, la Chine, l'Inde et Cuba ont reconnu qu'ils se préparent à la cyberguerre et qu'ils cherchent à renforcer leurs compétences en matière d'OI. La Corée du Nord, la Libye, l'Iran, l'Irak et la Syrie possèdent déjà certaines connaissances dans le domaine. Malgré tout, peu de pays sont en mesure d'intégrer les différents outils disponibles pour lancer une attaque massive capable de paralyser l'infrastructure d'un pays. Cela dit, certains pourraient y parvenir d'ici une dizaine d'années.

11. Le 7 février 2001, dans le discours sur la sécurité nationale (*Worldwide Threat 2001: National Security in a Changing World*) qu'il a prononcé devant le Select Committee on Intelligence du Sénat américain, le directeur de la CIA, George J. Tenet, a affirmé que les nouvelles technologies de communication facilitaient le travail des terroristes en les aidant à recueillir des fonds, à répandre leur dogme, à trouver des recrues et à planifier des opérations. Il a ajouté que certains groupes se dotent d'outils rudimentaires leur permettant de mener des cyberattaques. C'est Internet qui aide les groupes terroristes à adopter une structure organisationnelle sans dirigeant.

Sécurité des systèmes et des données

12. La conception d'outils et de techniques utiles aux OI progresse au même rythme que la technologie dans l'industrie des communications et de l'informatique. La possibilité de communiquer et de se brancher presque instantanément à des réseaux outre-mer comporte des avantages, mais rend aussi les systèmes plus vulnérables.

---

[7] Un "**cheval de Troie**" est un logiciel destructif ayant l'apparence d'une application bénigne. À l'encontre d'un virus, il ne peut se reproduire. Un **virus** est un code de logiciel qui se reproduit en se greffant à un autre programme. Il peut directement endommager certaines données ou encore dégrader la performance du système en s'emparant des ressources du système, qui n'est plus disponible aux utilisateurs autorisés. Un **ver** est un programme ou un élément de code de logiciel qui se trouve dans des réseaux ou des systèmes distribués. Il se multiplie afin de monopoliser le plus possible les resources du système pour ses propres besoins de traitement, ce qui a pour effet progressif de congestionner les réseaux et les systèmes informatiques.

13. Comme des intrus ont pénétré dans leurs réseaux, leur faisant ainsi perdre des informations sensibles, les gouvernements et les entreprises du monde entier ont tenté de mettre en oeuvre des mesures de sécurité pour protéger à la fois leurs systèmes et les données qu'ils contiennent. Malheureusement, ces mesures deviennent vite désuètes. Selon des enquêtes menées par des ministères et des entreprises de sécurité du secteur privé dans le monde, un grand nombre des dispositifs de sécurité et des outils de surveillance, qu'on trouve pour la plupart sur le marché, sont inefficaces ou mal configurés. Beaucoup d'enquêtes ont été menées aux États-Unis et au Royaume-Uni. Elles ont montré que plus de 80 pour 100 des répondants n'utilisaient pas de coupe-feux ni aucune autre mesure de sécurité pour protéger leurs systèmes et leurs données. Une autre enquête a révélé que jusqu'à 93 pour 100 des répondants étaient vulnérables à des attaques élémentaires, même si leurs systèmes étaient munis de coupe-feux.

14. Comme de plus en plus de personnes, d'entreprises et de ministères dépendent maintenant des communications informatisées et de l'exploitation de réseaux, la configuration des réseaux informatiques et des systèmes d'exploitation devient de plus en plus complexe, créant ainsi des failles. Les phénomènes naturels (comme les tempêtes), la création normale de logiciels et de nouveau matériel ainsi que les outils liés aux OI pourraient mettre à rude épreuve les failles des systèmes et causer des pannes susceptibles d'avoir des conséquences graves à court comme à long terme sur le bon fonctionnement du gouvernement et du secteur privé.

15. Dans son discours devant un sous-comité du Congrès, le directeur d'Internet Security Alliance a souligné que 80 pour 100 des failles importantes en matière de sécurité sont communes à toutes les organisations, ce qui s'explique en grande partie par le fait qu'elles utilisent les mêmes logiciels vulnérables. En règle générale, la capacité de créer des réseaux dépasse de loin celle d'assurer leur protection. Les entreprises du secteur privé, y compris certaines sociétés responsables de l'infrastructure essentielle, installent et utilisent des réseaux sans fil pour faciliter leurs activités. Non seulement beaucoup de ces systèmes n'ont pas une configuration sûre, mais ils prêtent aussi le flanc à l'exploitation.

Exemples d'opérations d'information

16. L'expérience des départements américains nous offre un bon nombre d'exemples d'OI et nous donne une idée de la façon de faire obstacle aux intrusions et à l'exploitation des systèmes. Ces incidents ont été relatés dans des discours prononcés devant des comités du Sénat et du Congrès et dans des documents produits par le General Accounting Office des États-Unis.

17. Certains groupes extrémistes, certaines organisations criminelles et certains gouvernements acquièrent des connaissances dans le domaine des OI et pourraient représenter une menace pour divers systèmes s'ils possédaient les techniques et les outils appropriés pour exploiter leurs failles et s'ils avaient la volonté de le faire. Les témoignages livrés devant les membres de certains comités du gouvernement américain ont révélé qu'un nombre croissant de pays possèdent ou tentent de mettre au point des programmes offensifs d'OI. De plus, des données indiquent qu'un nombre croissant de groupes extrémistes et de services de renseignements se familiarisent avec la conception et l'utilisation des outils et des techniques utiles aux OI. Plusieurs d'entre eux pourraient avoir l'intention d'utiliser ces outils pour se livrer à des activités traditionnelles qui représentent une menace.

18. Récemment, les médias ont annoncé que des pirates s'étaient introduits sans peine dans les réseaux militaires protégés des États-Unis à l'aide d'outils logiciels élémentaires. Les études du General Accounting Office ont montré que les outils logiciels offerts sur les sites Web de pirates informatiques

peuvent non seulement nuire aux opérations des départements américains, mais aussi menacer l'infrastructure essentielle du pays. D'après un rapport récent du National Institute of Standards and Technology, les pirates placent de 30 à 40 nouveaux outils sur leurs sites Web chaque mois. L'examen des statistiques indique qu'il y a eu 22 379 actes de sabotage de sites Web en 2001 et, des 29 000 actes répertoriés de 1998 au 22 janvier 2002, on compte 868 actes de sabotage contre des sites portant un « nom de domaine » américain, 519 dans le cas du Royaume-Uni, 345 dans celui de l'Australie et 205 pour ce qui est du Canada[8]. Ces données sont incomplètes puisque les victimes ne rapportent pas toujours les actes de sabotage et les autres attaques commises, mais l'information révèle une tendance, c'est-à-dire que le nombre d'intrusions est à la hausse.

19. En février 2000, un virus et des attaques décentralisées de déni de service ont perturbé certaines infrastructures nationales. Ces attaques, qui se concentraient sur un certain nombre d'entreprises très présentes sur Internet, ont causé, selon les estimations, des dommages de l'ordre de milliards de dollars. L'incident a prouvé que lorsque les pirates arrivent à parasiter un certain nombre d'ordinateurs, ils peuvent aller plus loin et utiliser tous les appareils simultanément pour concentrer leurs attaques sur une ou plusieurs cibles.

20. Par la suite, la propagation planétaire du virus « I Love You » a eu un effet encore plus grave sur les systèmes et les réseaux. Le phénomène est en partie attribuable à la phrase apparaissant comme sujet du courriel, c'est-à-dire « I Love You », une ruse bien pensée visant à inciter le plus de gens possible à ouvrir la pièce jointe infectée, contaminant ainsi leur système informatique. Les menaces numériques que représentent les virus, les vers et les chevaux de Troie entraînent des milliards de dollars de dommages chaque année. Selon les estimations de Computer Economics, une entreprise spécialisée dans les études de marché, les dommages se sont élevés à 17,1 milliards de dollars américains[9] en 2000 et à 13,2 milliards de dollars américains en 2001.

21. En 1997, les États-Unis ont évalué les risques qui pèsent sur l'industrie de l'électricité, ce qui leur a permis de se rendre compte que le réseau d'alimentation était criblé de points faibles. Certains éléments du réseau reposaient sur des systèmes non protégés de supervision, de contrôle et d'acquisition des données (SCADA)[10] auxquels les initiés pouvaient avoir accès en passant par les réseaux locaux intégrés. Dans d'autres cas, des systèmes SCADA non protégés pouvaient être contrôlés à distance par téléphone : il suffisait de connaître les numéros de téléphone nécessaires pour y accéder et compromettre le fonctionnement du réseau.

22. En 2001, Vitek Boden a été reconnu coupable en Australie d'utilisation de technologies sans fil pour pirater des ordinateurs équipés d'un système SCADA servant à contrôler certaines fonctions d'une

---

[8] Ces statistiques sont incomplètes puisqu'elles n'incluent que les actes de sabotage ayant été rapportés. Certains actes de sabotage et certaines formes de compromission et d'exploitation de systèmes ne sont pas rapportés et/ou consignés. Les statistiques pour les différents « noms de domaines » mentionnés ci-dessus ne comprennent pas le « .com », le « .net », le « .org », le « .edu » et les autres noms qui n'appartiennent à aucun pays en particulier.

[9] Le montant des dommages est élevé en 2000 en raison des conséquences du virus « I Love You ».

[10] SCADA est une application logicielle utilisée pour recueillir des données à distance en temps réel et traiter les données de manière à contrôler l'équipement. Combinant matériel informatique et logiciels, les systèmes SCADA émettent des mises en garde lorsque les conditions d'opération présentent des risques. Ils sont utilisés pour l'exploitation des centrales électriques, le raffinement du pétrole et du gaz, les télécommunications, les transports ainsi que la gestion de l'eau et des déchets.

station d'épuration des eaux usées. Au début de 2000, ses activités avaient entraîné le rejet d'eaux usées dans des réseaux d'aqueduc municipaux. On estime qu'il s'agit du premier cas connu de piratage « sans fil ». Les systèmes SCADA servent à contrôler toute une panoplie de procédés en lien avec l'infrastructure essentielle, comme la distribution de l'énergie électrique, le transport du gaz naturel ainsi que les services d'égouts et d'approvisionnement en eau partout dans le monde, y compris au Canada.

23. Dans divers pays, des tensions politiques et régionales ont été à l'origine de duels entre groupes de pirates informatiques :

- En 1999, des pirates du Japon et de la Chine se sont livrés bataille au sujet du massacre de Nankin.
- En Chine et à Taïwan, des pirates en sont venus à un véritable bras de fer sur la question de l'indépendance de Taïwan.
- La possession du Cachemire s'est avérée un enjeu de taille pour des pirates indiens et pakistanais.
- En 2000, des Arméniens ont placé de fausses informations dans un quotidien d'Azerbaïdjan, le *Zerkalo*.
- En 1999-2000, les tensions entre Israël et la Palestine ont amené des partisans des deux camps à se livrer à des actes de piratage, les partisans de la Palestine prenant même pour cible certaines entreprises et une organisation nord-américaine en faveur d'Israël.
- Des partisans de l'ancienne République de Yougoslavie ont lancé des attaques (virus et déni de service) contre des ordinateurs de l'OTAN.
- La collision entre un avion de surveillance des États-Unis et un chasseur de la Chine en avril 2001 a entraîné un duel entre pirates américains et chinois.
- L'Alliance musulmane Al Qaida, un regroupement de pirates appartenant au groupe pakistanais G-Force, au Pakistan Hackerz Club et à l'Anti-India Crew qui semble appuyer l'Al Qaida et embrasser la cause palestinienne, a piraté un certain nombre de sites américains, y compris celui du General Accounting Office, et a menacé de continuer ses attaques contre des sites indiens, américains et israéliens.

24. Les cyberattaques semblent être le résultat de tensions régionales et/ou d'attentats physiques commis par des groupes hostiles. En plus de prendre de l'ampleur, les attaques informatiques à motifs politiques sont de plus en plus sophistiquées et de mieux en mieux coordonnées.

Protection de l'infrastructure essentielle du Canada

25. Publié en 1999, le rapport du Comité spécial du Sénat sur la sécurité et les services de renseignements traite de la protection de l'infrastructure essentielle du Canada, à savoir des systèmes matériels et informatiques essentiels au bon fonctionnement quotidien de l'économie et du gouvernement. Par le passé, les éléments de cette infrastructure n'étaient pas réunis. Mais, peu à peu, ils ont été réunis, reliés, et sont devenus plus interdépendants. Les progrès de l'informatique et des communications ont présidé à une informatisation accrue des systèmes essentiels. Selon le rapport, la croissance de l'infrastructure essentielle, sa complexité et notre dépendance accrue à son égard en font une cible possible pour le terrorisme, qu'il soit matériel ou informatique.

26. Dans ses recommandations, le Comité suggère au gouvernement de prendre les mesures qui s'imposent pour protéger son infrastructure essentielle :

- concevoir des politiques et dégager des ressources permettant de faire face à n'importe quel type d'attaque;
- se doter de moyens permettant d'évaluer les points faibles de l'infrastructure, de la renforcer, de prévenir les attaques matérielles ou informatiques et, le cas échéant, d'intervenir;
- créer un partenariat entre les secteurs public et privé;
- veiller à l'évaluation et à la mise à jour régulières du Plan national de lutte contre le terrorisme, tout particulièrement en ce qui concerne l'incidence des nouvelles technologies susceptibles d'être utilisées par les terroristes.

27. À l'instar d'autres pays, le Canada a créé récemment un nouvel organisme chargé de protéger son infrastructure électronique contre les attaques informatiques et les désastres naturels. Ce nouvel organisme, appelé Bureau de la protection de l'infrastructure essentielle et de la planification d'urgence, relèvera du ministre de la Défense nationale et collaborera avec le ministère du Solliciteur général, les provinces, les municipalités, l'industrie privée et les autres pays.

Contexte découlant du 11 septembre

28. Les attentats terroristes du 11 septembre ont transformé le dossier de la protection de l'infrastructure essentielle. L'urgence est la même, mais les pays en sont davantage conscients. Les États-Unis ont créé plusieurs nouveaux organismes et adopté de nouvelles lois afin de renforcer la « sécurité intérieure », un concept visant la défense du territoire, de l'infrastructure essentielle et de la population. Le Canada, le Royaume-Uni et l'Australie ont élaboré ou adopté des lois antiterrorisme semblables. Corollaire de cette sensibilisation accrue à la sécurité, on commence à retirer de plusieurs sites Web des informations (données sur les plans d'urgence et l'emplacement de l'infrastructure essentielle) pouvant être utiles aux terroristes. Dans l'ensemble, les pays s'intéressent aujourd'hui davantage aux risques que constituent tous les types de cyberactivité pour la sécurité nationale. Ce que d'aucuns considéraient comme abstrait est maintenant perçu par certains comme possible et même probable.

Perspective

29. L'une des plus grandes difficultés que pose la lutte contre les OI, c'est l'inexistence des frontières pour quiconque travaille dans un environnement virtuel. Même si l'on travaillait d'arrache-pied pour éliminer toutes les failles, ce serait pratiquement peine perdue puisque les outils servant aux attaques, les réseaux et les systèmes qui gèrent ces réseaux évoluent sans cesse.

30. Au fur et à mesure que de nouvelles technologies voient le jour, de nouveaux outils et de nouvelles techniques d'attaque apparaissent. Par conséquent, les gouvernements devront mettre en oeuvre des procédures grâce auxquelles les dispositifs de sécurité suivront le pas des nouvelles menaces. Par exemple, le gouvernement en ligne, le passage au commerce électronique pour les entreprises, le désir du secteur privé d'offrir des services et de relier des systèmes à l'aide d'outils sans fil ainsi que l'utilisation de communicateurs personnels comportent tous des risques pour la sécurité.

31. Il est possible de réduire le nombre de points faibles des systèmes informatiques, mais on ne peut les éliminer entièrement. Ainsi, les systèmes qui ne disposent pas d'une solide protection continueront d'être infiltrés et exploités. En règle générale, les outils et les techniques servant à mener de telles attaques sont maintenant plus faciles à utiliser et leur mode d'opération est plus sophistiqué. Une multitude de groupes malveillants semblent chercher à améliorer leurs capacités en matière d'OI, lesquelles pourraient prendre une ampleur importante dans un proche avenir.

Perspectives est publié par la Direction de la recherche, de l'analyse et de la production du SCRS. Veuillez adresser tout commentaire concernant les publications au Directeur général, Direction de la recherche, de l'analyse et de la production à l'adresse suivante: C.P. 9732, Succursale T, Ottawa, (Ontario) K1G 4G4; ou par télécopieur au (613) 842-1312.